```
SHOW FILES; DS
File   2:INSPEC 1969-2002/Jan W1
         (c) 2002 Institution of Electrical Engineers
File   6:NTIS 1964-2002/Jan W3
         (c) 2002 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1970-2002/Jan W1
         (c) 2002 Engineering Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2002/Jan W1
         (c) 2002 Inst for Sci Info
File  35:Dissertation Abs Online 1861-2002/Jan
         (c) 2002 ProQuest Info&Learning
File  65:Inside Conferences 1993-2002/Jan W1
         (c) 2002 BLDSC all rts. reserv.
File  77:Conference Papers Index 1973-2002/Jan
         (c) 2002 Cambridge Sci Abs
File  92:IHS Intl.Stds.& Specs. 1999/Nov
         (c) 1999 Information Handling Services
File  94:JICST-EPlus 1985-2002/Nov W4
         (c)2002 Japan Science and Tech Corp(JST)
File  95:TEME-Technology & Management 1989-2002/JAN W1
         (c) 2002 FIZ TECHNIK
File  99:Wilson Appl. Sci & Tech Abs 1983-2001/Nov
         (c) 2001 The HW Wilson Co.
File 103:Energy SciTec 1974-2001/Sep B2
         (c) 2001 Contains copyrighted material
File 108:AEROSPACE DATABASE 1962-2001/DEC
         (c) 2001 AIAA
File 144:Pascal 1973-2002/Dec W5
         (c) 2002 INIST/CNRS
File 202:Information Science Abs. 1966-2001/ISSUE 09
         (c) Information Today, Inc
File 233:Internet & Personal Comp. Abs. 1981-2002/Jan
         (c) 2002 Info. Today Inc.
File 238:Abs. in New Tech & Eng. 1981-2001/Dec
         (c) 2001 Reed-Elsevier (UK) Ltd.
File 239:Mathsci 1940-2001/Feb
         (c) 2001 American Mathematical Society
File 275:Gale Group Computer DB(TM) 1983-2002/Jan 08
         (c) 2002 The Gale Group
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File 647:CMP  Computer Fulltext 1988-2002/Dec W4
         (c) 2002 CMP Media, LLC
File 674:Computer News Fulltext 1989-2001/Dec W2
         (c) 2001 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2002/Jan 08
         (c) 2002 The Dialog Corp.
File   9:Business & Industry(R) Jul/1994-2002/Jan 08
         (c) 2002 Resp. DB Svcs.
File  15:ABI/Inform(R) 1971-2002/Jan 07
         (c) 2002 ProQuest Info&Learning
File  16:Gale Group PROMT(R) 1990-2002/Jan 07
         (c) 2002 The Gale Group
File  18:Gale Group F&S Index(R) 1988-2002/Jan 04
         (c) 2002 The Gale Group
File  20:Dialog Global Reporter 1997-2002/Jan 08
         (c) 2002 The Dialog Corp.
File  80:TGG Aerospace/Def.Mkts(R) 1986-2002/Jan 07
         (c) 2002 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2002/Jan 04
         (c)2002 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 256:SoftBase:Reviews,Companies&Prods. 85-2002/Dec
         (c)2002 Info.Sources Inc
```

```
File 481:DELPHES Eur Bus 95-2002/Dec W3
         (c) 2002 ACFCI & Chambre CommInd Paris
File 583:Gale Group Globalbase(TM) 1986-2002/Jan 08
         (c) 2002 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2002/Jan 07
         (c) 2002 The Gale Group
File 624:McGraw-Hill Publications 1985-2002/Jan 08
         (c) 2002 McGraw-Hill Co. Inc
File 635:Business Dateline(R) 1985-2002/Jan 08
         (c) 2002 ProQuest Info&Learning

Set     Items   Description
S1         95   (HASH OR AUTHENTIC? OR MERKLE) (W) TREE?
S2       6725   (REVOCATION OR REVOK? OR EXPIR?) (5N) CERTIFICAT?
S3         15   S2 AND S1
S4          9   RD S3 (unique items)
?
```

T S4/FULL/1-9

**4/9/1 (Item 1 from file: 2)**
DIALOG(R)File 2:INSPEC
(c) 2002 Institution of Electrical Engineers. All rts. reserv.

7112544 INSPEC Abstract Number: B2002-01-6120D-087, C2002-01-1260C-069
**Title: Certificate revocation protocol using k-ary hash tree**
Author(s): Kikuchi, H.; Abe, K.; Nakanishi, S.
Author Affiliation: Dept. of Electr. Eng., Tokai Univ., Hiratsuka, Japan
Journal: IEICE Transactions on Communications vol.E84-B, no.8 p. 2026-32
Publisher: Inst. Electron. Inf. & Commun. Eng,
Publication Date: Aug. 2001 Country of Publication: Japan
CODEN: ITCMEZ ISSN: 0916-8516
SICI: 0916-8516(200108)E84B:8L.2026:CRPU;1-2
Material Identity Number: P711-2001-011
Language: English Document Type: Journal Paper (JP)
Treatment: Theoretical (T)
Abstract: Certificate revocation is a critical issue for a practical, public-key infrastructure. A new efficient revocation protocol using a one-way hash tree structure (instead of the classical list structure, which is known as a standard for revocation), was proposed and examined to reduce communication and computation costs. We analysis a k-ary hash tree for certificate revocation and prove that k=2 minimizes communication cost. ( 22 Refs)
Subfile: B C
Descriptors: certification; message authentication; protocols; public key cryptography; tree data structures
Identifiers: certificate revocation protocol; k-ary hash tree; public-key infrastructure; communication cost minimization
Class Codes: B6120D (Cryptography); B6150M (Protocols); C1260C ( Cryptography theory); C6130S (Data security); C6120 (File organisation); C5640 (Protocols)
Copyright 2001, IEE

**4/9/2 (Item 2 from file: 2)**
DIALOG(R)File 2:INSPEC
(c) 2002 Institution of Electrical Engineers. All rts. reserv.

7094869 INSPEC Abstract Number: B2002-01-6120D-004, C2002-01-6130S-008
**Title: Threaded binary sorted hash trees solution scheme for certificate revocation problem**
Author(s): Wang Shang-ping; Mang Ya-ling; Wang Yu-min
Author Affiliation: Nat. Key Lab. on ISN, Xidian Univ., Xi'an, China
Journal: Journal of Software vol.12, no.9 p.1341-50
Publisher: Science Press,
Publication Date: Sept. 2001 Country of Publication: China
CODEN: RUXUEW ISSN: 1000-9825
SICI: 1000-9825(200109)12:9L.1341:TBSH;1-A
Material Identity Number: G255-2001-010
Language: Chinese Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: A new solution scheme called certificate revocation threaded binary sorted hash trees (CRTBSHT) for the certificate revocation problem in public key infrastructure (PKI) is proposed. Previous solution schemes include: traditional X.509 certificate system's certificate revocation lists (CRL), S. Micali's (1996) Certificate Revocation System (CRS), P. Kocher's (1998) Certificate Revocation Trees (CRT). and Naor-Nissim's 2-3 certificate revocation trees (2-3 CRT) (M. Naor and K. Nissim, 2000) but none is perfect. The new scheme keeps the best properties of CRT, i.e., it is easy to check or prove whether a certificate is revoked which only needs related path values but does not need the whole CRT values and overcomes the disadvantage of CRT that any update will cause the whole CRT to be

computed completely. The new scheme has referential value to PKI engineering practice. (7 Refs)
Subfile: B C
Descriptors: certification; message authentication; public key cryptography; sorting; trees (mathematics)
Identifiers: threaded binary sorted hash tree solution scheme; certificate revocation problem; CRTBSHT; public key infrastructure; PKI; Certificate Revocation System; Certificate Revocation Trees; 2-3 certificate revocation tree; related path values; referential value; PKI engineering practice; certification authority; digital signature
Class Codes: B6120D (Cryptography); B0250 (Combinatorial mathematics); C6130S (Data security); C0310D (Computer installation management); C1160 ( Combinatorial mathematics)
Copyright 2001, IEE

**4/9/3 (Item 3 from file: 2)**
DIALOG(R)File 2:INSPEC
(c) 2002 Institution of Electrical Engineers. All rts. reserv.

6635492 INSPEC Abstract Number: B2000-08-6120D-015, C2000-08-6130S-021
**Title: Performance evaluation of certificate revocation using k-valued hash tree**
Author(s): Kikuchi, H.; Abe, K.; Nakanishi, S.
Author Affiliation: Dept. of Electr. Eng., Tokai Univ., Kanagawa, Japan
Conference Title: Information Security. Second International Workshop, ISW'99. Proceedings (Lecture Notes in Computer Science Vol.1729) p. 103-17
Editor(s): Mambo, M.; Zheng, Y.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 1999 Country of Publication: Germany ix+275 pp.
ISBN: 3 540 66695 8 Material Identity Number: XX-1999-03277
Conference Title: Information Security. Second International Workshop, ISW'99. Proceedings
Conference Date: 6-7 Nov. 1999 Conference Location: Kuala Lumpur, Malaysia
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: A CRL (certificate revocation list) defined in X.509 is currently used for certificate revocation. There are some issues of CRL including high communication cost and low latency for update. To solve the issues, there are many proposals including CRT (certificate revocation tree), authenticated dictionary, and delta list. In this paper, we study CRT using k-valued hash tree. To estimate the optimal value of k, we examine the overhead of computation and the communication cost. We also discuss when a CRT should be reduced by eliminating unnecessary entries that have already expired. (19 Refs)
Subfile: B C
Descriptors: certification; public key cryptography
Identifiers: performance evaluation; certificate revocation list; k-valued hash tree; X.509; update latency; communication cost; certificate revocation tree; authenticated dictionary; delta list; computation cost
Class Codes: B6120D (Cryptography); C6130S (Data security)
Copyright 2000, IEE

**4/9/4 (Item 4 from file: 2)**
DIALOG(R)File 2:INSPEC
(c) 2002 Institution of Electrical Engineers. All rts. reserv.

6396786 INSPEC Abstract Number: B1999-12-6120D-068, C1999-12-6130S-032
**Title: Performance evaluation of public-key certificate revocation system with balanced hash tree**
Author(s): Kikuchi, H.; Abe, K.; Nakanishi, S.

Author Affiliation: Tokai Univ., Kanagawa, Japan

Conference Title: Proceedings of the 1999 ICPP Workshops on Collaboration and Mobile Computing (CMC'99). Group Communications (IWGC). Internet '99 (IWI'99). Industrial Applications on Network Computing (INDAP). Multimedia Network Systems (MMNS). Security (IWSEC). Parallel Computing '99 (IWPC'99). Parallel Execution on Reconfigurable Hardware (PERH) p.204-9

Editor(s): Panda, D.; Takizawa, M.

Publisher: IEEE, Los Alamitos, CA, USA

Publication Date: 1999 Country of Publication: USA xxi+622 pp.

ISBN: 0 7695 0353 5 Material Identity Number: XX-1999-01656

U.S. Copyright Clearance Center Code: 0 7695 0353 5/99/$10.00

Conference Title: Proceedings of the 1999 ICPP Workshops

Conference Sponsor: Inf. Process. Soc. Japan (IPSJ); Int. Assoc. Comput. & Commun. (IACC); Univ. Aizu, Japan; Ohio State Univ., USA

Conference Date: 21-24 Sept. 1999 Conference Location: Aizu-Wakamatsu, Japan

Language: English Document Type: Conference Paper (PA)

Treatment: Applications (A); Practical (P)

Abstract: A new method for updating certificate revocation trees (CRT) is proposed. Efficient revocation of public-key certificates is a current issue in public-key infrastructure because a traditional certificate revocation list uses a large amount of bandwidth. A certificate revocation tree is a hash tree of revoiced certificates and reduces a bandwidth consumption up to O(log(n)). In this paper, an implementation of certificate revocation tree with S-expression is presented and the performance of the system is evaluated in terms of communication and computational costs. To update a CRT, we have two algorithms; (1) random insertion-a new certificate to be revoiced is just inserted into the existing tree and (2) balancing updating-balances CRT every time a new certificate is added. (7 Refs)

Subfile: B C

Descriptors: file organisation; performance evaluation; public key cryptography; tree data structures

Identifiers: performance evaluation; public-key certificate revocation system; balanced hash tree; public-key certificates; public-key infrastructure; certificate revocation tree; revoiced certificates; S-expression; random insertion

Class Codes: B6120D (Cryptography); C6130S (Data security); C6120 (File organisation); C5470 (Performance evaluation and testing); C5670 (Network performance)

Copyright 1999, IEE

**4/9/5 (Item 5 from file: 2)**

DIALOG(R)File 2:INSPEC

(c) 2002 Institution of Electrical Engineers. All rts. reserv.

6047572 INSPEC Abstract Number: B9811-6120B-102, C9811-6130S-098

**Title: On certificate revocation and validation**

Author(s): Kocher, P.C.

Author Affiliation: ValiCert, Palo Alto, CA, USA

Conference Title: Financial Cryptography. Second International Conference, FC'98 Proceedings p.172-7

Editor(s): Hirschfeld, R.

Publisher: Springer-Verlag, Berlin, Germany

Publication Date: 1998 Country of Publication: Germany viii+310 pp.

ISBN: 3 540 64951 4 Material Identity Number: XX98-02399

Conference Title: Financial Cryptography. Second International Conference, FC'98. Proceedings

Conference Date: 23-25 Feb. 1998 Conference Location: Anguilla

Language: English Document Type: Conference Paper (PA)

Treatment: Practical (P)

Abstract: Cryptosystems need to check whether the certificates and digital signatures they are given are valid before accepting them. In addition to providing cryptographically secure validity information, certificate revocation systems must satisfy a variety of challenging technical requirements. The traditional revocation techniques of certificate revocation lists (CRLs) and on-line checking are described, as well as a newer technique, certificate revocation trees (CRTs), based on Merkle hash trees. CRTs provide an efficient and highly-scalable way to distribute revocation information. CRT-based systems include tree issuers who compile revocation information. Confirmation issuers who distribute elements from CRTs, and users who accept certificates. CRTs are gaining increased use worldwide for several reasons. They can be used with existing protocols and certificates, and enable the secure, reliable, scalable, and inexpensive validation of certificates (as well as digital signatures and other data). (4 Refs)

Subfile: B C

Descriptors: certification; cryptography; protocols; tree data structures

Identifiers: certificate revocation; certificate validation; cryptosystems; digital signatures; cryptographically secure validity information; certificate revocation lists; on-line checking; certificate revocation trees; Merkle hash trees; revocation information distribution; tree issuers; revocation information compilation; protocols

Class Codes: B6120B (Codes); C6130S (Data security); C5640 (Protocols); C6120 (File organisation)

Copyright 1998, IEE

**4/9/6 (Item 1 from file: 94)**
DIALOG(R)File 94:JICST-EPlus
(c)2002 Japan Science and Tech Corp(JST). All rts. reserv.

04956300 JICST ACCESSION NUMBER: 01A0757710 FILE SEGMENT: JICST-E
**Internet Technology. Certificate Revocation Protocol Using k-Ary Hash Tree.**
KIKUCHI H (1); ABE K (1); NAKANISHI S (1)
(1) Tokai Univ., Hitatsuka-shi, Jpn
IEICE Trans Commun(Inst Electron Inf Commun Eng), 2001, VOL.E84-B,NO.8, PAGE.2026-2032, FIG.8, TBL.2, REF.22
JOURNAL NUMBER: L1369AAW ISSN NO: 0916-8516
UNIVERSAL DECIMAL CLASSIFICATION: 621.391.037.3
LANGUAGE: English COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Original paper
MEDIA TYPE: Printed Publication
ABSTRACT: Certificate Revocation is a critical issue for a practical, public-key infrastructure. A new efficient revocation protocol using a one-way hash tree structure (instead of the classical list structure, which is known as a standard for revocation), was proposed and examined to reduce communication and computation costs. In this paper, we analysis a k-ary hash tree for certificate revocation and prove that k=2 minimizes communication cost. (author abst.)
DESCRIPTORS: tree search; hash function; cryptography key; authentication; infrastructure; public key cryptography; protocol; computational complexity; cost analysis
BROADER DESCRIPTORS: function(mathematics); mapping(mathematics); cryptogram; rule; business analysis; analysis(separation); analysis
CLASSIFICATION CODE(S): ND02030R

**4/9/7 (Item 2 from file: 94)**
DIALOG(R)File 94:JICST-EPlus
(c)2002 Japan Science and Tech Corp(JST). All rts. reserv.

04636432 JICST ACCESSION NUMBER: 00A0625643 FILE SEGMENT: JICST-E
**Expected Reduction of Cost for Online Certification Status Verification With Red-Black Hash Tree.**
ABE KENSUKE (1); KIKUCHI HIROAKI (1); NAKANISHI SHOHACHIRO (1)
(1) Tokai Univ., Sch. of Eng.
Joho Shori Gakkai Kenkyu Hokoku, 2000, VOL.2000,NO.36(CSEC-9), PAGE.35-40,

FIG.6, TBL.4, REF.18
JOURNAL NUMBER: Z0031BAO    ISSN NO: 0919-6072
UNIVERSAL DECIMAL CLASSIFICATION: 681.3.02-759   681.3:007.51
LANGUAGE: Japanese        COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Original paper
MEDIA TYPE: Printed Publication

ABSTRACT: Certificate Revocation is one of the critical issues for a practical public-key infrastructure. A new efficient revocation protocol using one-way hash tree structure instead of the classical list structure, which is known as a standard for revocation, was proposed and examined in communication and computation costs reduction KA00!. A tree approach, however, might be of O(n) in the worst case when all entries are sorted in descending order. A red-black tree is a binary sorted tree with one extra bit per node, which is used for balancing tree and to guarantee that operations of search and insertion take O(log2 n) in the worst case. In this paper, we study the red-black hash tree for online certificate status verification and estimate the reduction of costs against the binary search tree in terms of communication and computation costs in revocation. (author abst.)

DESCRIPTORS: public key cryptography; binary search; computational complexity; hash function; packaging design; fast algorithm; speedup; performance analysis
IDENTIFIERS: calculation amount
BROADER DESCRIPTORS: cryptogram; tree search; function(mathematics); mapping(mathematics); design; computer algorithm; algorithm; modification; improvement; analysis
CLASSIFICATION CODE(S): JD01020V; JE08000Z

**4/9/8     (Item 3 from file: 94)**
DIALOG(R)File  94:JICST-EPlus

04615435   JICST ACCESSION NUMBER: 00A0430671  FILE SEGMENT: JICST-E

**Online Certificate Status Verification Server Using Binary Search Hash Tree.**

ABE KENSUKE (1); KIKUCHI HIROAKI (1); NAKANISHI SHOHACHIRO (1)
(1) Tokai Univ., Sch. of Eng.

Joho Shori Gakkai Kenkyu Hokoku, 2000, VOL.2000,NO.30(DPS-97 CSEC-8), PAGE.131-136, FIG.8, TBL.2, REF.17
JOURNAL NUMBER: Z0031BAO    ISSN NO: 0919-6072
UNIVERSAL DECIMAL CLASSIFICATION: 681.3.02-759
LANGUAGE: Japanese        COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Original paper
MEDIA TYPE: Printed Publication

ABSTRACT: CRT(Certificate Revocation Tree) is a method using hash tree for public-key certificate revocation. In  KA98!, we have implemented an experimental CRT system using the S-expression, and shown that its communication cost is smaller than that of CRL. In this paper, we implement an online certificate status verification server using CRT expressed in binary search tree, and examine the system performance in comparison with  KA98!. Based on experimental data, we show that the latency of CRT is smaller than that of CRL. We also estimate the performance of the system to which an actual revocation data derived from a CRL is applied. (author abst.)

DESCRIPTORS: data protection; hashing; authentication; packaging design; tree structure; telecommunication; client server system; speedup; performance evaluation; tree search; binary tree; main memory; cache memory
IDENTIFIERS: Java
BROADER DESCRIPTORS: protection; storage system; method; design; structure; computer system(hardware); system; modification; improvement; evaluation; tree(graph); subgraph; graph; memory(computer); equipment

```
CLASSIFICATION CODE(S): JD01020V


 4/9/9     (Item 4 from file: 94)
DIALOG(R)File  94:JICST-EPlus
(c)2002 Japan Science and Tech Corp(JST). All rts. reserv.

03792520   JICST ACCESSION NUMBER: 98A0986994  FILE SEGMENT: JICST-E
Certificate Revocation and Update Using Binary Hash Tree.
KIKUCHI HIROAKI (1); ABE KENSUKE (1); NAKANISHI SHOHACHIRO (1)
(1) Tokai Univ., Sch. of Eng.
Joho Shori Gakkai Kenkyu Hokoku, 1998, VOL.98,NO.84(DPS-90 CSEC-2),
    PAGE.51-56, FIG.9, REF.8
JOURNAL NUMBER: Z0031BAO    ISSN NO: 0919-6072
UNIVERSAL DECIMAL CLASSIFICATION: 681.3.02-759   621.391.037.3
LANGUAGE: Japanese         COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Original paper
MEDIA TYPE: Printed Publication
ABSTRACT: A CRL(Certificate Revocation List) defined in X.509 is currently
    used for revocation. To corp with issue of CRL,  that includes a high
    communication cost and low latency for update, OCSP, Delta-CRL,
    CRT(Certificate Revocation Tree) and Authenticated Directory have been
    proposed. In this paper, we implement experimental CRT system, and the
    expected reduction of communication cost in comparison with CRL. We
    also propose a new update method which is more efficient in
    communication than Naor's evaluate method. (author abst.)
DESCRIPTORS: computer security; public key cryptography; data update;
    hashing; binary tree; performance evaluation; data protection
BROADER DESCRIPTORS: security; guarantee; cryptogram; renewal; storage
    system; method; tree(graph); subgraph; graph; evaluation; protection
CLASSIFICATION CODE(S): JD01020V; ND02030R
?
```